AN ANALYSIS OF BLOCKCHAIN-BASED CLOUD STORAGE SYSTEM WITH QUALITY IMPROVEMENT

#1RAMAKRISHNA VEMULA, Research Scholar,
#2Dr. ANOOP SHARMA, Guide,
Department of Computer Science & Engineering,
UNIVERSITY OF TECHNOLOGY, JAIPUR, RAJASTHAN
Corresponding Author: *Ramakrishna Vemula*, vemula.ramakrishna@yahoo.com

ABSTRACT: The significance of Blockchain innovation has served as a driving force for both scholarly and practical investigation. The ongoing development of the blockchain technology presents a promising solution to various technological hurdles, encompassing decentralization, identification, trust, integrity, data ownership, and information-driven decision-making. The exponential growth of digital data is being driven by both automatic systems and human users. The utilization of blockchain technology plays a crucial role in the assessment and selection of the optimal cloud storage and processing alternative. This article provides an analysis of the security implications associated with the utilization of blockchain technology in the context of cloud storage..

Keywords: *Block chain Technology, Distributed cloud storage system, Feature selection*

1. INTRODUCTION

Everyone is talking about “the cloud” now. People are talking about cloud computing, despite the metaphor. Future apps should stay in the cloud now. Cloud computing supports many business applications and client needs. Dell EMC and Amazon choose cloud-based services over traditional data centers due to their cost and technical sophistication.

Security is the biggest drawback of any storage method. Moving firm data to the cloud requires supplier data security. Due to overlapping trust boundaries and increasing data exposure, malicious cloud consumers might attack IT systems and steal business data.

The blockchain-based “Distributed cloud model” can tackle cloud security issues. Popular blockchain users want secure, cost-effective ways to store their growing data libraries. Blockchain for Bitcoin reduces third-party trust. Blockchain database is decentralized. Hacking is practically impossible with a visible, traceable peer-to-peer system.

2. RELATED WORK

Blockchain

Blockchain technology mixes previously unrelated technologies in a novel way. The Internet, private key cryptography, and the distributed open ledger protocol are all examples of technologies. To simplify Blockchain, consider using an example. A, B, C, and D are four entities/nodes that want to transfer money. A has ten dollars and transfers five dollars to B, three dollars to C, and one dollar to D.

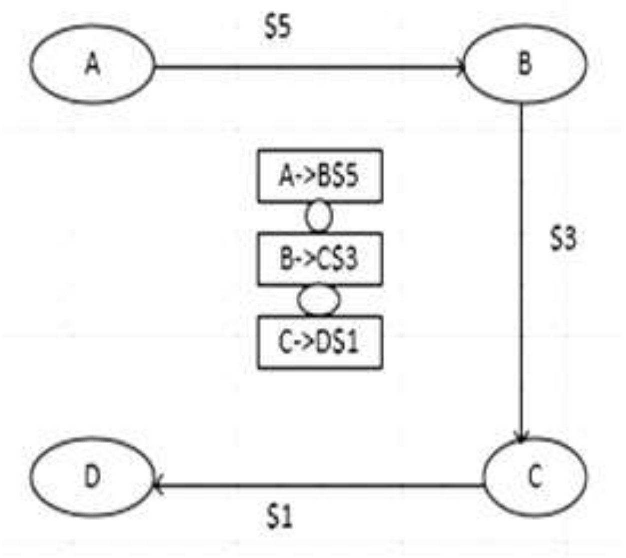

Fig1:OpenLedgerProtocol

All of these transactions are centrally recorded and linked, and all entities are aware of them. The protocol described above is an open ledger protocol, and a "ledger" is a record that contains all of the transactions. Each transaction is known and verified by all parties. If D requires $15 from A, A cannot transfer it since it has only $5 remaining, and all of the other entities are aware of this. The primary distinction is that the data, i.e. transactions, are not held centrally in blockchain, but each organization will have a copy.

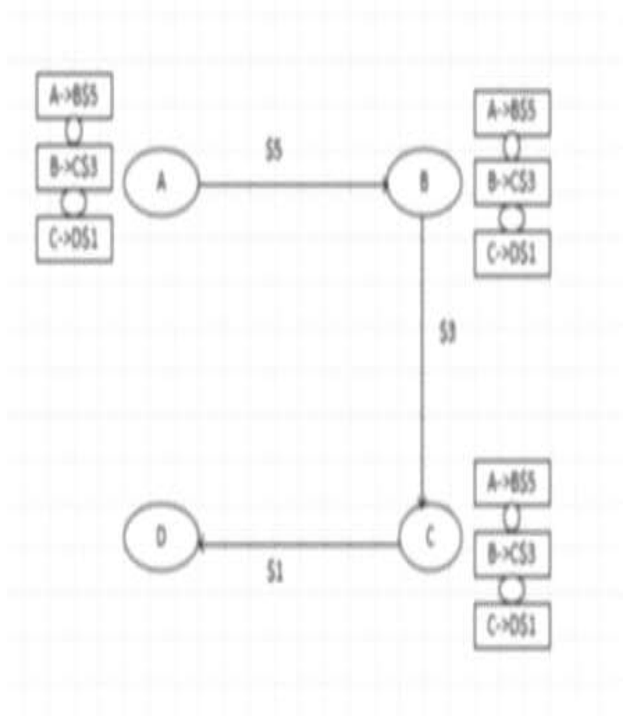

Fig2:DistributedOpenLedgerProtocol

By distributing data over its network, the blockchain avoids the risks associated with centrally stored data. Blockchain security methods employ public-key cryptography. That address is associated with value tokens sent across the network. A private key, like a password, provides access to the data to the owner. This is where blockchain technology comes into play. Everyone involved has access to decentralized data. In a decentralized system, the blockchain is copied on each node. To broadcast transactions to the network, software is employed. Mining nodes validate transactions, add them to the block in progress, and then broadcast the finished block to other nodes. This also keeps the various data versions that different nodes have in sync. Let's have a look at the prior example to see how this works.

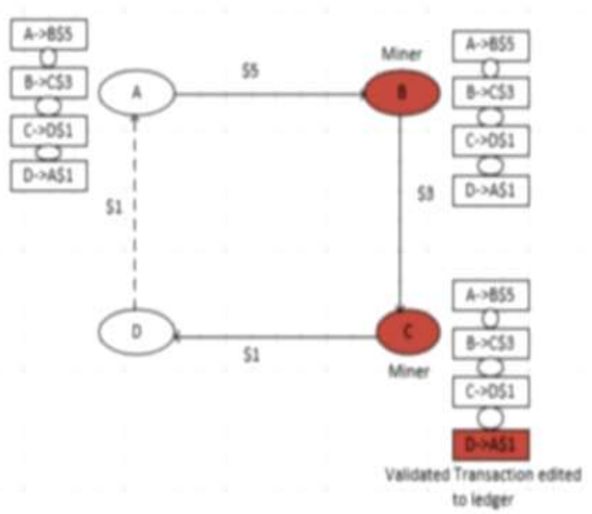

Fig3:Datatransactioninadistributedopenledger

Assume D wishes to send A $1. D encrypts the data with a public key and sends it to A, who has the private key, to be decoded and accessed. A broadcast message will be used to communicate this transaction to the network. A blockchain network will contain special nodes known as "miners" that will be able to validate a transaction. If C and B are the miners, they will try to validate the D-to-A transaction. In this case, two points can be utilized to validate. The public key is being decrypted if D has the requisite funds for this transaction. C and B are both aware that D has the funds to finish this transaction because every node in this network has a copy of the previous transactions. Decrypting the public key, on the other hand, is difficult; a miner generates keys repeatedly and attempts to guess the correct key until one is discovered. If C finds the key that corresponds to the key for this transaction, it validates it and adds it to its own ledger. All of the other nodes will do the same because this transaction has already been validated.

3. REVIEW OF LITERATURE

The anonymous person or group that is thought to be behind Bitcoin is called Satoshi Nakamoto. In a paper that was published in 2008, Satoshi Nakamoto detailed how the blockchain technology, which is a distributed peer-to-peer linked-structure, could be used to solve the problems of maintaining the order of transactions and preventing double spending. This technology is a distributed peer-to-peer linked-structure. This technique creates a linked-structure that is decentralized and peer-to-peer. Transactions are grouped and bundled together in a structure of a fixed size known as blocks in Bitcoin. This structure is called the blockchain. Due to the fact that these blocks all have the same history, they all have the same timestamp. According to Crosby et al. (2016), the nodes of the network, which are also known as miners, are the ones who are in charge of chronologically linking the blocks to one another. These nodes are also the ones who are responsible for maintaining the blockchain. Each new block that is added to a blockchain is required, as part of the process of building the blockchain, to contain the hash of the block that was added to the blockchain immediately prior to it. Because of this, the structure of the blockchain is in a position to store a trustworthy and verifiable ledger of all of the transactions that take place across the network.

The proliferation of blockchain technology has caused huge upheavals to occur in the conventional methods of carrying out corporate transactions. This is as a result of the fact that apps and transactions that previously relied on centralized systems or trusted third parties for verification are now able to run in a decentralized manner while still maintaining the same level of confidence. This is the result of the fact that blockchain technology has advanced. This is possible as a direct result of the innovation brought about by the blockchain technology. principles such as transparency, resilience, auditability, and security are provided by the fundamental principles of blockchain architecture and design (Greenspan, 2015a; Christidis & Devetsikiotis, 2016). Blockchains are distributed ledgers that use cryptography to record transactions and verify their authenticity. Blockchains are a type of decentralized ledger that record transactions in a public and chronological order. Blockchain technology is what enables these traits to be utilized. One way to think of a blockchain is as a decentralized database that takes the shape of a list of blocks that are arranged in a specific way. Consider a blockchain in this light as one way to think about it. After a block has been added to the chain, any changes that were previously made to that block will no longer be available. Given that many financial institutions would be able to coordinate their activities within the same blockchain and push transactions on behalf of their own customers, it is easy to understand why this would be helpful for the financial sector. It is easy to understand why this would be beneficial for the financial business. In this manner, the technology that underpins blockchain can make auditing financial transactions much simpler. Blockchain already makes it possible to ensure that transactions are transparent. Companies make investments in this technology because they believe it has the potential to enable them to decentralize their infrastructures and reduce the costs of their transactions while at the same time making transactions intrinsically safer, more transparent, and in some cases even quicker. Companies make these investments because they believe this technology has the potential to enable them to do all of these things. Blockchain is the name given to this type of technology. The investigation leads one to the conclusion that the blockchain technology is more than a passing fad.

The fact that there are presently more than 1900 distinct cryptocurrencies is evidence of the relevance of Blockchain, as stated by CoinMarketCap (2017). It is expected that this number will continue to climb in the coming years. According to Tschorsch and Scheuermann (2016) and Haferkorn and Quintana Diaz (2015), the rapid development of cryptocurrency applications may swiftly lead to the emergence of interoperability issues. This is due to the fact that different cryptocurrency applications serve different purposes. In addition, the landscape is going through a rapid change as a result of the growth of blockchain technology beyond the realm of cryptocurrencies, with smart contracts (SCs) playing a major role. This is causing the landscape to undergo a rapid transformation. Because of this, the landscape is undergoing a significant change at an accelerated rate. SCs, which were first described by Szabo in 1994 as "a computerized transaction protocol that executes the terms of a contract" (Szabo, 1994), provide us with the capability of translating contractual clauses into code that can be embedded (Szabo, 1997). This, in turn, reduces the amount of external participation and the risks that are associated with it. In light of the previous discussion, a self-executing contract (SC) is an agreement between parties in which the terms of the agreement are automatically enforced, despite the fact that the parties do not trust each other. This is the definition of a self-executing contract. Smart contracts (SCs), as defined by Christidis and Devetsikiotis (2016), are scripts that run in a decentralized way and are stored on blockchains. This definition relates to programmable "smart contracts" in the context of blockchain technology. These programs don't rely on any trustworthy information source at all, therefore they're quite useless. In particular, blockchain-based systems that permit SCs make it possible for more sophisticated processes and interactions, which results in the generation of a new paradigm that can be applied to virtually a limitless number of situations. Blockchains are decentralized databases that can be used to record transactions across multiple computers.

This is one of the key reasons why the use of Blockchain technology is becoming increasingly significant, as stated by Zhao et al. (2016). More than one-third of executives working in C-suite roles have reportedly said that they are either considering embracing blockchains or have already begun doing so, according to a study that was carried out by IBM (2017). These CEOs were interviewed, and from those interviews, this information was collected. According to Christidis and Devetsikiotis (2016), researchers and developers are already familiar with the potential of the new technology, and they are exploring various applications across a wide variety of industries. Christidis and Devetsikiotis also state that the potential of the new technology has already been researched and developed. Christidis and Devetsikiotis both indicate that research and development work has already been done on the prospective applications of the new technology. According to Zhao et al. (2016), there have been three generations of blockchains that may be separated from one another based on the distinct types of users that each blockchain is designed for. These generations are as follows: Blockchain 1.0 offers programs that make it possible to conduct transactions using digital currencies. Blockchain 2.0 introduces the concept of smart contracts as well as a collection of applications that go beyond simple cryptocurrency exchanges. Blockchain 3.0 incorporates applications in domains that go beyond those of the previous two generations, such as the internet of things, the government, the medical field, and scientific research. Blockchain 1.0 offers programs that make it possible to conduct transactions using digital currencies. Smart contracts will be included in Blockchain 2.0. Applications are a component of Blockchain 3.0.

Even though there have been a number of studies conducted on blockchain technology (Tama et al., 2017; Brando et al., 2018), we believe that the current state of the art in blockchain-enabled applications has gotten insufficient attention. This is because there have been a number of studies conducted on blockchain technology. These reviews are available for your perusal here and here, respectively. Even in Zheng et al. (2016), the applications of blockchains are not studied to their full degree, nor are they addressed in a manner that is applicable. This is the case even though Zheng et al. (2016) was written. In addition, Zheng et al. (2016) does not offer any examples to support their claims. There are some reviews that are focused on the specific role that blockchain plays, such as the development of decentralized and data-intensive applications for the Internet of Things (Conoscenti et al., 2016; Christidis and

Devetsikiotis, 2016), and managing big data in a decentralized manner (Karafiloski and Mishev, 2017a). In addition, there are some reviews that are focused on the general role that blockchain plays in the industry. In addition, there are other reviews that concentrate on the possible uses of blockchain technology. Other studies concentrate on the blockchain's ability to promote trust and decentralization in service systems (Seebacher et al., 2017) and P2P platforms (Hawlitschek et al., 2018), as well as its potential vulnerabilities in the field of information security (Khan and Salah, 2017; Li et al., 2017a; Meng et al., 2018). Khan and Salah (2017) as well as Li et al. (2017)a have found that. Several technical aspects of the blockchain's design, such as its consensus protocol (Sankar et al., 2017) and the vulnerabilities of SCs (Atzei et al., 2017), as well as other technical characteristics such as its size and bandwidth, usability, data integrity, and scalability, have been investigated by Yli-Huumo et al. (2016) and Koteska et al. (2017), respectively. Koteska et al. The blockchain technology has also been the subject of some of these researchers' investigations. In addition, there are more studies, such as Bonneau et al. (2015), Tsukerman (2015), Mukhopadhyay et al. (2016), Khalilov and Levi (2018), and Conti et al. (2018), that are more focused on the financial side of blockchains in addition to the security and privacy that they provide.

In light of recent research, blockchain networks have been categorized in a broad variety of different ways. Buterin (2015), Zheng et al. (2016), Eris Industries (2016), Christidis and Devetsikiotis (2016), Kravchenko (2016), and Wood (2016) are some examples of this type of research. When the administration and rights criteria of a network are implemented, the three types of networks that result are public, private, and federated. The distinction between a public blockchain and a permissionless blockchain is that anyone can join a public blockchain as a new user or a node miner. A public blockchain is the same thing as a permissionless blockchain. In addition, each and every member of the group is given the authority to carry out activities such as transactions and contracts independently of the others in the group. In private blockchains, which are also known as permissioned blockchains and federated blockchains, there is typically a whitelist of permitted users that is established with particular characteristics and permissions over the operations of the network. This whitelist of permitted users has certain characteristics and permissions over the transactions that take place on the blockchain. The activities that take place on the blockchain can therefore be controlled in a more granular fashion as a result of this. The term "federated blockchains" refers to a group of blockchains that also includes these private blockchains. According to Swanson (2015), private blockchain networks are able to eliminate the need for costly PoW algorithms because the likelihood of Sybil assaults occurring on these networks is essentially nonexistent. Instead, one alternative that might be taken into account is the adoption of a larger variety of consensus protocols that are founded on disincentives. This is because it is an alternative that has the potential to be more effective. According to the definitions provided by Buterin (2015) and Zheng et al. (2016), a federated blockchain is a type of hybrid blockchain that brings together public and private blockchains. The validation of transaction processes is not performed by a single entity but rather outsourced to a group of nodes known as "leader nodes." This eliminates the need to rely on a central authority. This is the primary distinction that can be made between a public blockchain and a private blockchain, despite the fact that both kinds of blockchains provide a same level of scalability and protection for users' privacy. As a consequence of this, it is now possible to create an architecture that is only partially centralized and in which leader nodes are able to delegate authorization obligations to other users. This opens up a lot of new possibilities. In this paper, we provide a classification of blockchain networks that is more fine-grained than the existing state-of-the-art (Buterin, 2015; Zheng et al., 2016; Christidis and Devetsikiotis, 2016; Kravchenko, 2016) (Buterin, 2015; Zheng et al., 2016; Christidis and Devetsikiotis, 2016; Kravchenko, 2016). Kravchenko and Christidis (2016); Christidis and Devetsikiotis (2016). This is because in addition to more conventional aspects such as the ownership and management of the information that is shared in the blockchain, we also take into consideration features such as the length of time it takes for a transaction to be approved, in addition to aspects of security such as anonymity. This is why this is the case.

Bitcoin, Ethereum, and Litecoin are a few well-known implementations of public blockchains (Nakamoto, 2008; Haferkorn and Quintana Diaz, 2015). Other examples include Hyperledger Fabric and Quorum. A few examples of cryptocurrencies include Bitcoin, Ethereum, and Litecoin. The decentralized ledger known as blockchain is used by the overwhelming majority of cryptocurrencies now in circulation. One of the most important advantages connected with them is the absence of costs associated with the infrastructure; this is one of the most significant perks. Because the network is capable of becoming self-sufficient and maintaining itself, there is a significant reduction in the amount of overhead costs related with management. This is because of the fact that the network is able to sustain itself. According to Zheng et al. (2016), the key applications for private blockchains include database management, auditing, and more broadly, solutions that place a high value on performance. These are thought to be the most important applications for private blockchains. According to Greenspan (2015b), an example of an open platform that may be utilized for the establishment and operation of private blockchains is Multichain. According to research conducted by R3 in 2015, the banking and manufacturing sectors are the ones that utilize federated blockchains the most frequently. This is not the least significant factor to take into consideration. This is the situation that exists in regard to the Hyperledger project (Hyperledger Project, 2015), which creates permission-based blockchain frameworks that are applicable to a wide variety of various types of companies. Additionally, as of late, Ethereum has been offering tools that can be utilized in the creation of federated blockchains. These tools can be used in place of the original Ethereum blockchain. Other initiatives, such as Cardano (2018), have a much more ambitious objective of delivering more functionality, and they are putting a lot of effort into accomplishing this goal. Walport (2016) and Swanson (2015) are two sources that the reader might want to look into if they have an interest in gaining a deeper understanding of the various classifications that can be applied to blockchains. Both of these sources offer a great deal of data and information pertaining to the subject.

4. TRADITIONALCLOUDSTORAGE MODEL

A classic cloud storage model has a client or mobile device, a server or storage, and a network. Traditional cloud storage is Google Drive. Cloud data is kept at Google datacenters. Mobile devices/laptops request data from the data center.

Theproblem(s)

It is expensive to run massive data centers. These data centers require constant technological updates. Cooling, maintenance, and upgrades are examples of operational costs. Another consideration is safety. Despite the fact that all cloud service providers follow strong security standards, personal data can still be accessed. Recently, a celebrity cloud breach occurred. Human error is not the only threat to your privacy. Unencrypted files can be searched by large corporations. Their privacy policies detail the various ways they can lawfully access and share your information.

DistributedCloudStorage

The blockchain will house all cloud storage components, including data transmission, processing, and storage. Anyone with blockchain access can certify data fate. This solution gives the cloud full traceability, accountability, and transparency. Data can be stored securely and decentralized utilizing Distributed Cloud architecture. Blockchain technologies like ledgers, public/private key encryption, and others achieve this, as detailed earlier in this article. Users regain control over their data and devices with these features. The decentralized nature protects central servers.

DistributedCloudDesignConsiderations

These criteria should be considered while designing a high-performance distributed cloud architecture for present and future challenges:

Node resilience: Others compute if some fail. Nodes function well for users.

Easy deployment: Nodes can be deployed anywhere without affecting others.

Adaptability: Network architecture should adapt to client needs and the environment.

Distributed networks must perform linearly.

Address data, confidentiality, and information security.

Blockchain Distributed Cloud Architecture

The four-step model is suggested:

Distributed cloud blockchain consumers choose a service provider pool resource provider.

That supplier will provide user data management, task execution, and servers.

The service provider publishes the transaction on blockchain and shares it with all distributed peer service providers.

Payment: All peers record the user paying the service provider in their blockchain.

Trusted peer-to-peer network maintains distributed ledger with verifying nodes/miners that reply to requests. Client SDKs or REST APIs request. The ordering service gets approved results following peer reviews. After order consensus, peer nodes validate and append results to the ledger in cryptographically secure, tamper-proof data blocks.

Blockchain network members can join instantaneously, locally or worldwide. After creating an instance, exchange cryptographic certificates to join the blockchain and safely transact with peers. Undistributable business data is shared by members. Subnet peers and creates private ledgers. Blockchain coexisters can transact privately. Other chain organizations must approve peers to join. After approval, client requests are delivered to a channel and updated in its ledger, which only peer nodes may see.

5. BLOCKCHAIN ARCHITECTURE

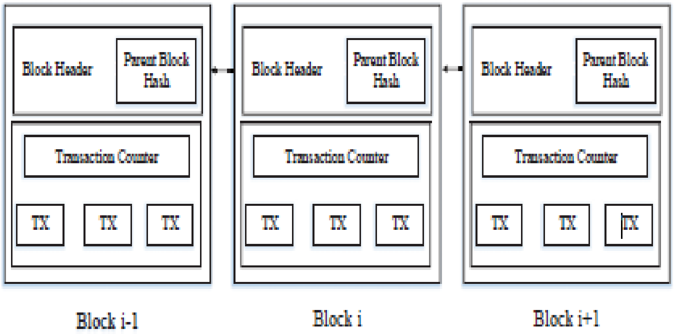

Fig. 4: A blockchain with continuous blocks.

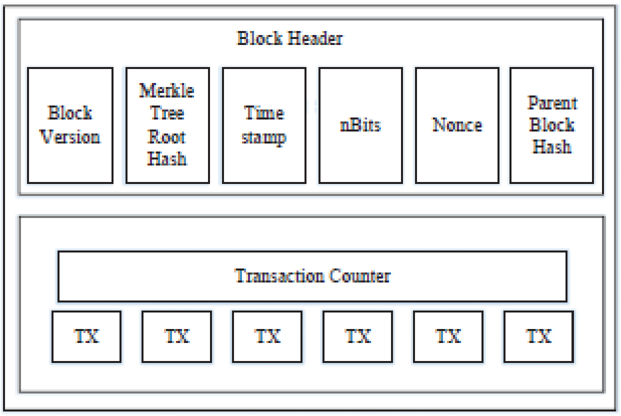

Fig. 5: Block structure

The blockchain is a sequential arrangement of blocks that acts as a repository for all transactional information, similar to a public ledger. The diagram in Figure 4 shows a representation of a blockchain. Block headers carry the hashes of the preceding blocks, establishing a hierarchical relationship in which each block has a single parent block. The insertion of hashes from uncle blocks into the Ethereum blockchain would be implemented. A blockchain's first block, known as the genesis block, has no preceding parent block. Following that, we will outline the internal workings of blockchain.

BLOCK

Figure 5 illustrates the header and body of a block. In particular, the block header:

- ➢ The term "block version" refers to the establishment of validation rules.
- ➢ The Merkle tree root hash represents the aggregation of all block transactions.
- ➢ The measurement of time in universal seconds has been in use since January 1, 1970.
- ➢ The value nBits represents the threshold for the block hash.
- ➢ The "Never" field is a 4-byte component that exhibits incremental growth with each subsequent hash calculation.

- The parent block hash refers to the 256-bit hash value of the preceding block.

The block body consists of transactions and a counter. The upper limit of transactions per block is contingent upon the dimensions of both the block and the individual transactions. The utilization of asymmetric cryptography is employed by blockchain technology for the purpose of transaction verification. Asymmetric cryptography digital signatures are employed in circumstances characterized by a lack of trustworthiness. Next, we will provide a concise overview of the concept of digital signatures.

DIGITAL SIGNATURE

Every user has a private and public key. The confidential private key signs transactions. The entire network broadcasts digitally signed transactions. The usual digital signature has two phases: signing and verification. For instance, Alice wishes to message Bob. (1) Alice encrypts her data with her private key and sends Bob the encrypted and original data during signing.

(2) Bob verifies the value with Alice's public key. Bob could easily check for data tampering. Blockchains typically use the elliptic curve digital signature algorithm.

KEY CHARACTERISTICS OF BLOCKCHAIN

Decentralization.

The central trusted agency (e.g., the central bank) validates each transaction in typical centralized transaction systems, causing central server cost and performance limitations. Blockchain does not require third parties like centralized mode. Blockchain consensus maintains data consistency in decentralized networks.

Persistency.

Transactions can be confirmed quickly, and honest miners reject invalid ones. Once in the blockchain, transactions are almost unreversible. Blocks with invalid transactions are promptly discovered.

Anonymity. Each user can interact with the blockchain using a hidden address.

Auditability. Bitcoin uses UTXO to store user balances: Transactions must reference unspent ones. Unspent transactions become spent after the current transaction is recorded in the blockchain. We could simply verify and track transactions.

TAXONOMY OF BLOCKCHAIN SYSTEMS

Three main blockchain systems are public, private, and consortium. Everyone can participate in consensus on public blockchain records. Only pre-selected nodes would reach consensus, unlike a consortium blockchain. Private blockchains allow only one organization's nodes to participate in consensus.

***Consensus determination*.**Public blockchains allow consensus from all nodes. Consortium blockchains validate blocks by select nodes. Private chains are managed by one organization that decides consensus.

Read permission. Private and consortium blockchain transactions are not public.

Immutability. Because many participants keep records, public blockchain transactions are nearly impossible to change. Because there are fewer players, private or consortium blockchain transactions can be tampered with.

Efficiency. Public blockchains require a lot of time to distribute transactions and blocks because of all the nodes involved. Due to increased transaction delays, throughput is reduced. A smaller number of validators may have benefits for consortium and private blockchains.

Centralized. Public, consortium, and private blockchains are decentralized, somewhat centralized, and fully centralized because they are held by one person.

Consensus process. Global consensus is possible on public blockchain. Private and permissioned consortium blockchains differ of public.

Since public blockchain is open to everyone, it has many users and active communities. Many public blockchains appear daily. Consortium blockchain has several commercial uses. Hyperledger creates corporate consortium blockchains. Ethereum offers consortium blockchains.

6. CONCLUSION

In this study, we have conducted a comprehensive analysis of the Traditional cloud model and its inherent constraints. During the discussion, the subject of blockchain technology was deliberated, with a specific focus on the development of a decentralized blockchain cloud infrastructure.

During the discourse, we examined the merits of this specific entity and deliberated upon a multitude of prospective applications for it. Based on the projections provided by Cisco, it is anticipated that the quantity of internet-connected devices will have a growth rate above 100% by the year 2020, ultimately surpassing the threshold of 50 billion. The observed rise in connectivity indicates a corresponding surge in the production of online content, hence creating a heightened need for secure storage options. The current cloud paradigm is inadequate in addressing future requirements. The possibility exists for a distributed cloud architecture that is robustly constructed and accessible to the public to supplant the tasks currently performed by cloud intermediaries. The responsibilities encompass establishing a reliable trade environment, mitigating occurrences of fraudulent activities and misuse, and ensuring compliance with contractual obligations and secure financial transactions. The utilization of blockchain technology in the context of distributed cloud storage endeavors to offer an innovative resolution to an escalating issue. We are currently on the verge of reaching a critical juncture that could have severe and adverse consequences. Numerous individuals establish comparisons between blockchain technology and the nascent phase of the internet during the 1990s, underscoring the potential of blockchain in a comparable manner.

REFERENCES

[1]. "Blockchain and Distributed Ledger Technology"https://www.sap.com/india/products/leonardo/blockchain.html#

[2]. Martin Korling "Future Digital Blog" http://cloudblog.ericsson.com/digital-services/distributed-cloud-infrastructure-nfvJune12,2017

[3]. "Integrate Your Business Network with the Blockchain Platform"https://cloud.oracle.com/opc/paas/ebooks/Oracle_Blockchain_Cloud_Service.pdf

[4]. "How Blockchain Tech Is Changing Cloud Storage" https://www.belugacdn.com/blog/162663814938-how-blockchain-tech-is-changing-cloud-storage.

[5]. M. A. Harlev, H. Sun Yin, K. C. Langenheldt, R. R. Mukkamala, and R. Vatrapu, "Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning," in Proceedings of the 51st Hawaii International Conference on System Sciences, 01 2018.

[6]. P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak et al., "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," Oncotarget, vol. 9, no. 5, p. 5665, 2018.

[7]. The European Parliament, "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46 (general data protection regulation) [GDPR]," Official Journal of the European Union, vol. 59, no. L119, pp. 1–88, 05 2016.

[8]. G. Zyskind, O. Nathan et al., "Decentralizing privacy: Using blockchain to protect personal data," in Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, 2015, pp. 180–184.

[9]. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, no. 10, p. 218, 2016.

[10]. A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data," in Proceedings of IEEE open & big data conference, vol. 13, 2016, p. 13.

[11]. S. Chernbumroong, S. Cang, A. Atkins, and H. Yu, "Elderly activities recognition and classification for applications in assisted living," Expert Systems with Applications, vol. 40, no. 5, pp. 1662–1674, 2013.

[12]. C. A. Ronao and S.-B. Cho, "Human activity recognition with smart- phone sensors using deep learning neural networks," Expert

Systems with Applications, vol. 59, pp. 235–244, 2016.

[13]. C. Pulliam, S. Eichenseer, C. Goetz, O. Waln, C. Hunter, J. Jankovic, D. Vaillancourt, J. Giuffrida, and D. Heldman, “Continuous in-home monitoring of essential tremor,” Parkinsonism & related disorders, vol. 20, no. 1, pp. 37–40, 2014.

[14]. M. A. Alsheikh, A. Selim, D. Niyato, L. Doyle, S. Lin, and H.-P. Tan, “Deep activity recognition models with triaxial accelerometers.” in AAAI Workshop: Artificial Intelligence Applied to Assistive Technologies and Smart Environments, 2016.

[15]. M. Ermes, J.Pa¨rkka¨, J.Ma¨ntyja¨rvi, and I. Korhonen, “Detection of daily activities and sports with wearable sensors in controlled and uncontrolled conditions,” IEEE transactions on information technology in biomedicine, vol. 12, no. 1, pp. 20–26, 2008.